4 Estrategias para la Creación de un Plan de Concienciación

No existe una única estrategia válida para todas las organizaciones. La elección correcta dependerá de la madurez de la empresa, su cultura, su tamaño, su sector y los riesgos específicos a los que se enfrenta.

Como arquitectos del plan, vuestra primera decisión es definir el **enfoque estratégico**. Podemos clasificar las estrategias más comunes según tres ejes principales:

4.1 Eje de actuación 1: La Frecuencia (Cuándo)

1. **Estrategia "Big Bang" (o Campaña Anual)**
    - **Características:** Es el enfoque tradicional. Consiste en una gran campaña de formación una vez al año (a menudo en un mes específico, como el "Mes de la Ciberseguridad"). Todos los empleados deben completar un módulo de eLearning extenso (30-60 minutos).
    - **Ventajas:**
        - **Cumplimiento:** Es la forma más fácil de "marcar la casilla" y demostrar a los auditores que el 100% del personal ha recibido formación.
        - **Gestión Sencilla:** Fácil de planificar y ejecutar logísticamente.
    - **Desventajas:**
        - **Curva del Olvido:** La información se olvida casi por completo pasados dos meses.
        - **Rechazo del Empleado:** Se percibe como una tarea pesada y aburrida, generando "fatiga formativa".
        - **Ineficaz:** No produce un cambio de comportamiento real.
2. **Estrategia "Always-On" (o de Goteo Continuo)**
    - **Características:** Es el enfoque moderno. En lugar de un gran evento, la formación se distribuye a lo largo del año en pequeñas dosis (microlearning). Esto se combina con simulaciones de phishing frecuentes pero aleatorias.
    - **Ventajas:**
        - **Retención:** Mantiene la ciberseguridad "top of mind" (en la mente de todos) constantemente.

- **Cambio de Comportamiento:** Refuerza los hábitos de forma continua.
- **Menos Intrusivo:** Un vídeo de 3 minutos al mes es mejor aceptado que un curso de 1 hora al año.

- **Desventajas:**
  - **Más Complejo:** Requiere una planificación continua y una plataforma que lo gestione.

4.2 Eje de actuación 2: La Segmentación (A quién)

1. **Estrategia Universal ("One-Size-Fits-All")**
   - **Características:** Todos los empleados de la organización reciben exactamente el mismo contenido formativo, independientemente de su rol, departamento o nivel de acceso.
   - **Ventajas:**
     - **Simplicidad:** Extremadamente fácil de administrar.
     - **Línea Base:** Asegura que todos tengan un nivel mínimo de conocimiento.
   - **Desventajas:**
     - **Irrelevante:** El contenido genérico aburre. El equipo de Finanzas no se siente identificado con los riesgos de un técnico de campo, y viceversa.
     - **Poca Eficacia:** Los empleados desconectan si no perciben el riesgo como algo relevante para su trabajo diario.
2. **Estrategia Basada en Riesgo y Roles (Segmentada)**
   - **Características:** El plan se diseña en función del riesgo. Se identifica a los grupos de mayor riesgo y se les asigna formación específica.
   - **Segmentación Típica:**
     - **VAPs (Very Attacked People):** ¿Quiénes son los más atacados? (Ej. Directivos, sus asistentes, RR. HH., Finanzas).
     - **Roles Críticos:** ¿Quiénes tienen acceso a los datos más sensibles? (Ej. Administradores de IT, desarrolladores con acceso a producción).
     - **Riesgo Específico:** El equipo de Finanzas recibe formación avanzada sobre fraude BEC (Business Email Compromise) y suplantación de facturas. El equipo de RR. HH. recibe formación sobre CVs con malware.
   - **Ventajas:**
     - **Máxima Relevancia:** El empleado siente que la formación está hecha para él.
     - **Eficiencia:** Se invierten los recursos en mitigar los riesgos más grandes.

- **Desventajas:**
    - **Requiere Análisis Previo:** Necesitáis saber dónde están vuestros riesgos antes de empezar.

4.3 Eje de actuación 3: El Tono y la Motivación (Cómo)

1. **Estrategia Punitiva ("El Palo")**
    - **Características:** Se enfoca en el castigo. El empleado que falla una simulación de phishing es penalizado: debe repetir un curso, su mánager es notificado, o incluso se vincula a su evaluación de desempeño.
    - **Ventajas:**
        - **Resultados Rápidos (Aparentes):** El miedo puede reducir la tasa de clics a corto plazo.
    - **Desventajas:**
        - **Genera una Cultura Tóxica:** Los empleados desarrollan miedo y resentimiento hacia el departamento de Seguridad.
        - **Ocultación de Incidentes: Este es el mayor peligro.** Si un empleado hace clic en un phishing real, tendrá miedo de reportarlo, dando tiempo al atacante. Fomenta el "borrar y callar".
2. **Estrategia de Refuerzo Positivo ("La Zanahoria")**
    - **Características:** Se enfoca en premiar el buen comportamiento. Se utiliza la **gamificación** (puntos, insignias) y el reconocimiento público.
    - **Ejemplos:**
        - Se premia a los empleados que **reportan** correos sospechosos (la métrica clave).
        - Se crean "campeones de seguridad" (*Security Champions*) en cada departamento.
        - Se publican tablas de clasificación de los departamentos más "seguros".
    - **Ventajas:**
        - **Alto Engagement:** Los empleados participan voluntariamente.
        - **Fomenta el Reporte:** Se crea una alianza entre los empleados y Seguridad.
        - **Sostenible a Largo Plazo:** Construye una verdadera cultura de seguridad.
    - **Desventajas:**
        - Requiere más creatividad y un esfuerzo de comunicación constante.

4.4 Recomendación de actuación: La Estrategia Híbrida Moderna

La estrategia más eficaz hoy en día no es una u otra, sino una **combinación inteligente**:

- **Frecuencia: Continua (Always-On)**, usando microlearning y simulaciones frecuentes para reforzar.
- **Base de Cumplimiento:** Complementada con un módulo **anual** más extenso para cubrir los aspectos legales (RGPD, políticas internas) y establecer la línea base.
- **Segmentación: Basada en Riesgo**, con un núcleo común para todos, pero con módulos específicos y simulaciones más difíciles para los grupos VAP.
- **Tono: Refuerzo Positivo**, midiendo y premiando la *tasa de reportes* por encima de la *tasa de clics*. El objetivo no es que no fallen, sino que sepan qué hacer cuando fallan o sospechan.